International Journal of Digital Crime and Forensics
Volume 13 • Issue 3 • Bi-Monthly 2021

A HEVC Video Steganalysis Against DCT/DST-Based Steganography

Henan Shi, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Tanfeng Sun, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Xinghao Jiang, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Yi Dong, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Ke Xu, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

ABSTRACT

The development of video steganography has put forward a higher demand for video steganalysis. This paper presents a novel steganalysis against discrete cosine/sine transform (DCT/DST)-based steganography for high efficiency video coding (HEVC) videos. The new steganalysis employs special frames extraction (SFE) and accordion unfolding (AU) transformation to target the latest DCT/DST domain HEVC video steganography algorithms by merging temporal and spatial correlation. In this article, the distortion process of DCT/DST-based HEVC steganography is firstly analyzed. Then, based on the analysis, two kinds of distortion, the intra-frame distortion and the inter-frame distortion, are mainly caused by DCT/DST-based steganography. Finally, to effectively detect these distortions, an innovative method of HEVC steganalysis is proposed, which gives a combination feature of SFE and a temporal to spatial transformation, AU. The experiment results show that the proposed steganalysis performs better than other methods.

KEYWORDS

AU, DCT/DST, Distortion, HEVC, SFE, Spatial Correlation, Temporal Correlation, Video Steganalysis, Video Steganography

INTRODUCTION

Modern steganography is an art and science of covert communication. It is a technology that protect the secret data from discovered or theft (Mishra et al., 2015). As a new method to ensure communication security in the network environment, steganography technology has received extensive attention. As a counter-technique to it, the goal of steganalysis is to detect the presence of hidden data in a cover object. Research on video steganalysis technology is not only to cope with the development of video steganography technology, but also has important significance to national security and public safety.

In modern steganography, the object can be images, videos, documents, sound files etc. Using documents and images as secret message carriers has yielded rich results in the current steganographic research field, but the structure of text and image is simple and the chance of exposure is more. In contrast, video carrier, as an emerging mainstream digital media exploding on the network, has the characteristics of high capacity and insensitivity to distortion. Using videos as carries of secret message has higher value in the field of information hiding. According to the research, over a quarter

DOI: 10.4018/IJDCF.20210501.oa2

of internet traffic is used up by video stream transmissions (Price, 2011). Besides, HEVC, as the most recent video standard, is developed in the pursuit of better compression performance relative to H.264 standard, achieving the range of 50% bit-rate reduction for equal perceptual video quality (Sullivan et al., 2012). It is well adapted for network transmission. In view of the aforementioned facts, steganalysis in HEVC videos is of paramount importance.

Up to date steganalysis methods are usually by detecting the modification of certain coding coefficients, such as motion vectors (MV) (Deng et al., 2012; Tasdemir et al., 2016; Wang et al., 2015), prediction modes (Li et al., 2014; Sheng et al., 2017; Zhao et al., 2015) and quantized DCT coefficients (Rabee et al., 2017; Wang et al., 2017). This paper focuses on DCT/DST domain steganalysis. The research of steganography using quantized DCT coefficients has been well studied in image steganography and H.264 video steganography. Rabee et al. (2017) presented a blind JPEG steganalysis based on DCT coefficients differneces, and Wang et al. (2017) proposed a steganalysis to detect DCT-based data hiding methods for H.264/AVC videos. However, both of them are not specialized in detecting DCT/DST domain steganography algorithms for HEVC videos. From another aspect, many steganalysis methods developed by exploiting the spatial or temporal correlation in video stream have been proposed. Tasdemir et al. (2015) proposed a HEVC steganalysis system utilizing temporal pixel correlation of videos. It employed Accordion Unfolding (AU) transformation and detected pixel domain image steganography algorithms used on video frames. Besides, Da et al. (2015) established markov model of inter-frames by using the gray-level co-occurrence matrix between blocks, implementing the combination of spatial correlation with temporal correlation among frames. Zarmehi et al. (2016) estimated the cover frames and computed features both from video frames and residual matrix. Though few researches in attacking steganography algorithms proposed specially for HEVC videos, the steganalysis schemes above also inspire the design of the novel steganalysis.

In short, few studies focus on detecting DCT/DST-based steganography for HEVC videos, and DCT/DST domain steganography algorithms in HEVC lack targeted security detection. Therefore, previous works cannot be directly used to detect DCT/DST-based steganography for HEVC videos since unique techniques or distortion in HEVC are not considered.

To solve above problem, related theory analysis and experiments are done as well as a novel steganalysis. The contributions of this paper include: 1) Analysis on the distortion process of DCT/DST-based HEVC steganography. 2) A targeted steganalysis against DCT/DST-based steganography for HEVC videos.

The rest of this paper is organized as follows. Related works are introduced in Section 2 and analysis on the distortion process of DCT/DST-based HEVC steganography algorithms is presented is Section 3. In Section 4, proposed HEVC video steganalysis is explained. Section 5 shows the experimental results and experimental analysis. In Section 6, the conclusions and future works are given.

RELATED WORKS

Steganalysis techniques are developed to cope with the abuse of steganography. Nowadays, with the application of advanced video compression and network technology, the object of video has become one of the most popular online media, and it also has been one of the most suitable carriers for information hiding. Hence here are some introductions to related video steganography and steganalysis techniques.

Video steganography can be performed in pixel, DCT/DST, motion vectors, inner predictions of macro blocks etc. domains. In this paper, we deal with DCT/DST domain steganography. In DCT/DST-based steganography algorithms, secret data are covertly transmitted in the way of disturbing DCT/DST coefficients. For HEVC videos, Liu et al. (2018) presented a new steganography method for H.265/HEVC video streams without intra-frame distortion drift. It is the latest and the most advanced DCT/DST-based steganography algorithm in HEVC. In Liu et al. (2018), since human eyes

are less sensitive to the brightness, the steganography algorithm only embeds message into 4×4 blocks. Three conditions of the directions of intra-frame prediction and the multi-coefficients are given, and the steganography algorithm can avert intra-frame distortion drift and get good visual quality. Besides, Chang et al. (2014) proposed a DCT/DST-based error propagation-free steganography algorithm for HEVC intra-coded frames, which is also a commonly used DCT/DST domain steganography algorithm in HEVC. These two most prominent DCT/DST domain HEVC video steganography algorithms are both implemented to establish video data sets and tested with the proposed steganalysis method in this study.

However, though some of current studies have proposed methods for without intra-frame distortion drift steganography algorithms in H.264 and HEVC, for steganography the distortion of the value of pixel and inter-frame distortion drift etc. problems are still existed. In this paper, in view of existed problems in current DCT/DST-based steganography algorithms in HEVC, in order to design a more targeted and effective steganalysis method, the process of intra-fame distortion and inter-frame distortion are analyzed fully.

When compared to image steganalysis and H.264 video steganalysis, there are limited number of HEVC video steganalysis methods. As shown in Table 1, characteristics of related steganalysis methods are listed. As described in the first row of Table 1, Tasdemir et al. (2015) gave a steganalysis system utilizing temporal pixel correlation of HEVC video. It is one of the most commonly used and advanced steganalysis methods for HEVC. It employed Accordion Unfolding (AU) transformation in pixel domain video steganalysis, and temporal and spatial correlation were utilized together. With help of the AU transformation, temporal correlation was incorporated into the steganalysis system, and the temporal dependency substantially increased the detection accuracy (Tasdemir et al., 2015). Thus, in this study, the proposed novel steganalysis also uses the AU transformation to merge temporal and spatial correlation, and it makes full use of the temporal correlation among video frames. Besides, Fridrich & Kodovsky (2012) proposed Spatial Rich Model (SRM) for spatial steganalysis, which is the most influential example in the trend of employing many weak filters and obtaining high dimensional features. Diverse set of weak features given by it makes the detection of steganography more comprehensive and accurate. Therefore, spatial only steganalysis (Fridrich & Kodovsky, 2012) and only AU transformation based steganalysis (Tasdemir et al., 2015) are both implemented to detect several steganography algorithms for contrast with the proposed steganalysis.

However, the steganalysis system in Tasdemir et al. (2015) remains to be improved. Firstly, though it is one of the few steganalysis for HEVC videos, it just detected two spatial image steganography algorithms, WOW (Holub & Fridrich, 2012) and UNI (Holub et al., 2014), and it did not detect specific steganography algorithms in HEVC. Then, it caused other problems when using AU transformation only. When AU transformation is employed, some spatial correlation is destroyed, and detection of partial spatial correlation is lacked. In result, some trace of distortion caused by steganography cannot

Table 1. Characteristics of comparative steganalysis methods

Articles of Steganalysis	Feature Name	Performance	Insufficiency
A steganalysis system utilizing temporal pixel correlation of HEVC video (2015)	Features of SRM of AU transformed frames.	Suitable for video streams.	• Lack of experiments attacking HEVC video steganography algorithms. • Some spatial correlation of frames is destroyed when AU transformation is employed.
Rich models for steganalysis of digital images (2012)	Features of SRM of images.	Suitable for images.	• Applicable only to images. • High computational power and requirements for training time.

be captured, and the detection accuracy will be influenced. Therefore, the proposed steganalysis employs Special Frames Extraction (SFE) besides AU transformation to add the detection of spatial correlation, and it gets a higher detection accuracy.

DISTORTION PROCESS ANALYSIS

In this section, analysis of distortion process of DCT/DST-based HEVC steganography is introduced.

Analysis on Intra-Frame Distortion

First, the process of the HEVC transform and quantization is presented. As shown in Figure 1, intra predicted value of current block is obtained after intra estimation and intra prediction. HEVC specifies the Transform Unit (TU) for transform and quantization coding of the prediction residual. The prediction residual within the N×N TU for N = 32, 16, 8, 4 is denoted as $R^{P}_{N\times N}$. The output of transformation and quantization module, denoted as $R^{QDCT}_{N\times N}$ with N = 32, 16, 8 or $R^{QDST}_{4\times 4}$, is disturbed to embed hidden bits. For simplicity, the case that the TUs are of size 4×4 is explained as an example here. The QDST coefficient matrix of $R^{P}_{4\times 4}$ can be expressed as:

$$R^{QDST}_{4\times 4} = (HR^{P}_{4\times 4}H^{T})\times\frac{1}{Q} \tag{1}$$

where Q is the quantizer step size determined by a Quantization Parameter (QP) and

$$H=\begin{bmatrix} A & B & C & D \\ C & C & 0 & -C \\ D & -A & -C & B \\ B & -D & C & -A \end{bmatrix} \tag{2}$$

At the decoding stage, the reconstructed residual is obtained by performing inverse QDST (IQDST) on

$R^{QDST}_{4\times 4}$, which can be represented as:

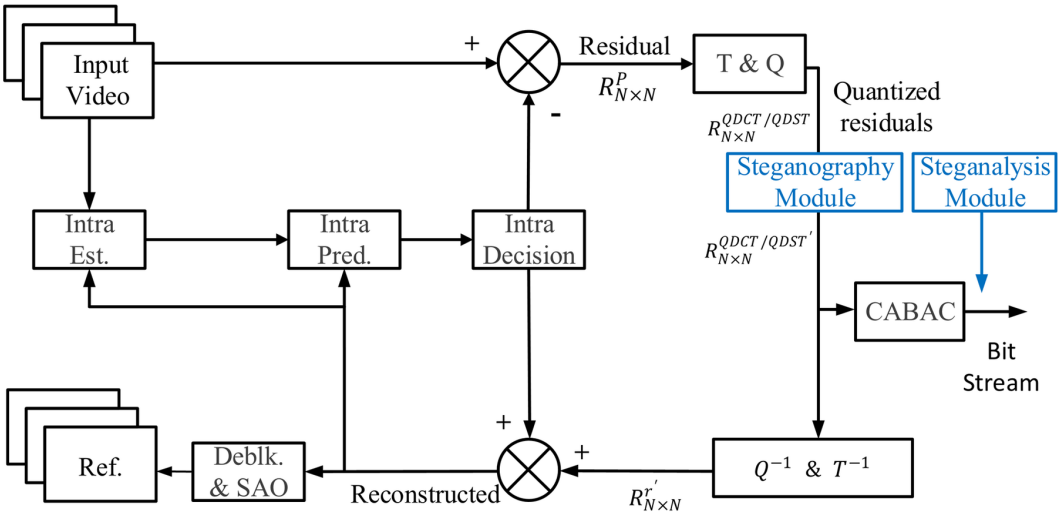
$$R^{r}_{4\times 4} = IQDST(R^{QDST}_{4\times 4}) = H^{-1}(R^{QDST}_{4\times 4}\times Q)(H^{T})^{-1} \tag{3}$$

where H^{-1} means the inverse matrix of H.

Based on the process of transform and quantization, the current DCT/DST-based HEVC steganography (Chang et al., 2014; Liu et al., 2018) are designed to prevent intra-frame error propagation. However, these DCT/DST-based HEVC steganography will still cause intra-frame distortion.

For intra-frame distortion, to analyze the effect of modifying DCT/DST on reconstruction values, a coefficients perturbing example in algorithm Chang et al. (2014) is presented to explain the steganography procedure and the corresponding distortion. Taking the 4×4 TU as an example, the embedding process is shown as:

Figure 1. DCT/DST-based steganography in HEVC intra coding process



$$\Delta R_{4\times4}^{QDST} = R_{4\times4}^{QDST'} - R_{4\times4}^{QDST} = \begin{bmatrix} m & 0 & -m & m \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

where m means secret message. The perturbed QDST coefficient matrix is denoted as $R_{4\times4}^{QDST'}$. After performing IQDST defined in Equation 3 on it, the reconstructed perturbed residual $R_{4\times4}^{r'}$ is obtained. The difference between it and $R_{4\times4}^{r}$ can be expressed as:

$$\Delta R_{4\times4}^{r} = R_{4\times4}^{r'} - R_{4\times4}^{r} = H^{-1}(\Delta R_{4\times4}^{QDST} \times Q)(H^{T})^{-1} = Q \times m \times \begin{bmatrix} 0 & 0 & 3AC & 0 \\ 0 & 0 & 3BC & 0 \\ 0 & 0 & 3C^{2} & 0 \\ 0 & 0 & 3CD & 0 \end{bmatrix} \tag{5}$$

As shown above, the rightmost column values are all 0, which means the current HEVC steganography algorithms Chang et al. (2014) and Liu et al. (2018) prevent intra-frame error propagation to right blocks. However, the third column values are changed. Consequently, the main intra-frame distortion is on the reconstructed value of the current block. The distortion is characterized as follows:

$$ERR_{intra} = \sum_{i=1}^{S} (\Delta R_{N\times N,i}^{r}) \tag{6}$$

where S denotes the number of all modified blocks in DCT/DST-based video steganography.

Analysis on Inter-Frame Distortion

For inter-frame distortion, the principle of HEVC inter-frame prediction is predicting pixels of the current frame using pixels of adjacent encoded I-frame or P-frame. P-frame uses forward estimation, expressed as:

$$RV_k^r = f_P(RV_{k-n_1}^r) \tag{7}$$

where $f_P(\cdot)$ denotes forward estimation and coding process in P-frame, RV_k^r presents the reconstruction value in k^{th} frame and n_1 is determined by reference frame. If the reconstruction values in the frame number of $k-n_1$ are modified due to DCT/DST-based steganography, the current reconstruction value will be perturbed, denoted as $RV_k^{r'}$. The distortion propagated to the k^{th} frame can be expressed as:

$$\Delta RV_k^r = RV_k^{r'} - RV_k^r = f_P(RV_{k-n_1}^{r'}) - f_P(RV_{k-n_1}^r) \tag{8}$$

Based on these equations, the intra-frame distortion in encoded reconstructed frames can propagate to pending encoding frames. B-frame uses bi-directional estimation, sharing similar inter-frame distortion. Assuming the number of inter-frame distortion propagated frames is M, the inter-frame distortion, ERR_{inter}, can be expressed as:

$$ERR_{\text{inter}} = \sum_{i=1}^{M}(\Delta RV_i^r) \tag{9}$$

In summary, both intra-frame distortion and inter-frame distortion are caused by DCT/DST-based HEVC steganography. Total distortions, ERR_t, can be expressed as follows:

$$ERR_t = ERR_{\text{intra}} + ERR_{\text{inter}} \tag{10}$$

Based on the above analysis, the intra-frame distortion and the inter-frame distortion introduced by this steganography will cause distortions in pixel domain, which are weak and distributed. Thus, to capture a large number of different types of dependencies among pixels, Spatial Rich Model (SRM) (Fridrich & Kodovsky, 2012) is used for detection in the proposed steganalysis.

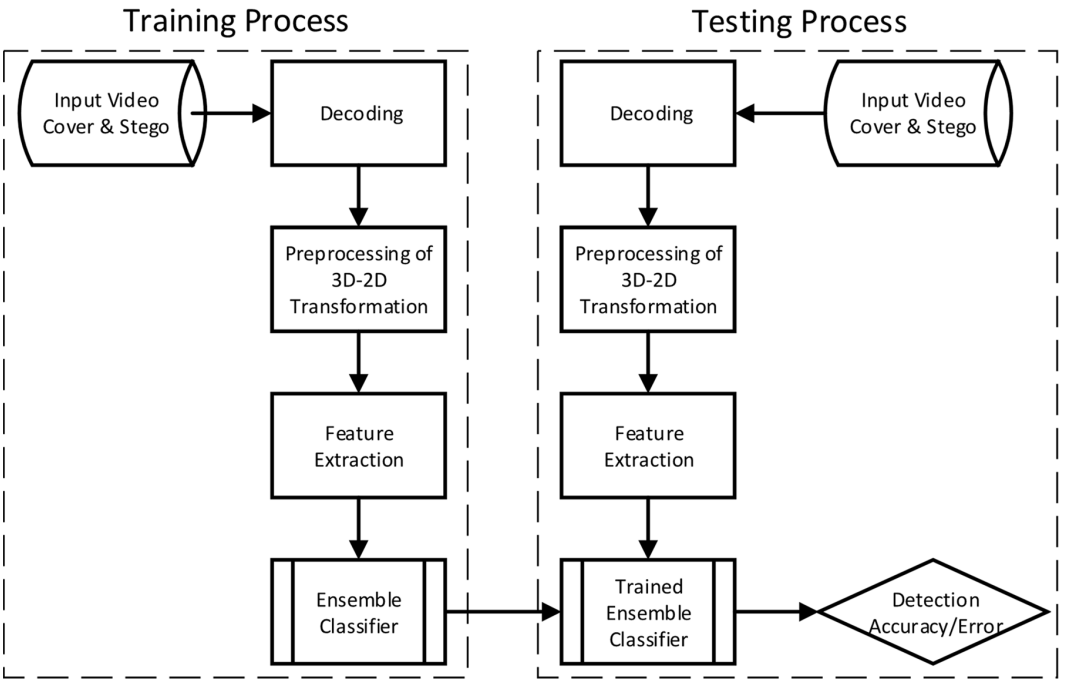
PROPOSED HEVC VIDEO STEGANALYSIS

Proposed steganalysis enhances the detections of temporal and spatial inter-pixel dependencies for these distortions. The framework is shown in Figure 2.

Preprocessing of 3D-2D Transformation

In this section, Accordion Unfolding (AU) and Special Frames Extraction (SFE) are described detailly and used to cope with inter-frame distortion and intra-frame distortion respectively.

Figure 2. Framework of the proposed steganalysis



Accordion Unfolding

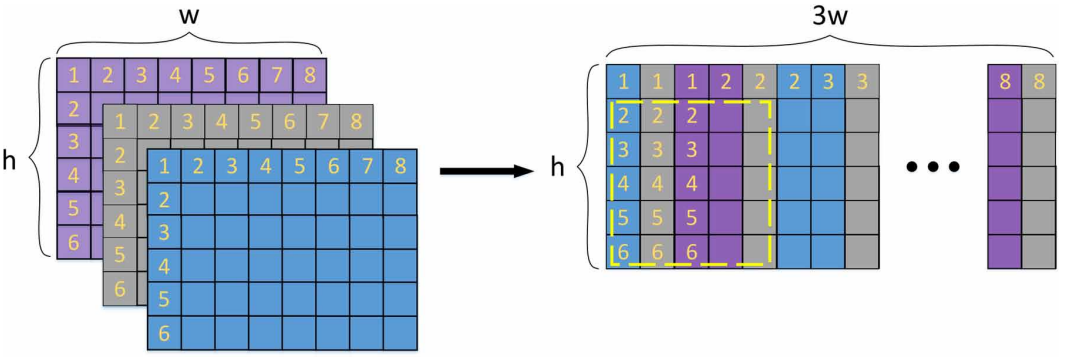
To detect the inter-frame distortion, AU is utilized in the proposed steganalysis method. AU was first developed for utilizing temporal dependency in motion vectors of a video (Tasdemir et al., 2015). The steps of it are shown in Figure 3. Three consequent frames, F_{k-1}, F_k and F_{k+1}, are temporally concatenated, forming a frames block. Then, first columns of reconstruction value RV^r in F_{k-1}, F_k and F_{k+1} are glued together. Second columns of F_{k+1}, F_k and F_{k-1} are glued subsequently. The final unfolded frame, $F_{k_1}^{'}$, is obtained. Thus, temporal dependencies are preserved in the final unfolded frames, and filters can capture both spatial and temporal correlation.

However, the transformation of AU causes a longer distance between half of horizontally adjacent pixels in a frame, which means the 5×5 kernel filter with the largest coverage in SRM (Fridrich & Kodovsky, 2012), as depicted with dashed square in Figure 3, fails in capturing dependencies among those pixels. Thus, in the way of only employing AU transformation in preprocessing of 3D-2D transformation, intra-frame distortion will not be detected accurately.

Special Frames Extraction

SFE is proposed for solving above problem and enhancing the detection of intra-frame distortion. As shown in Figure 4, SFE and AU are depicted in black and blue respectively. Secret message are embedded only in I-frames for DCT/DST-based video steganography, so I-frames, $F_{k_2}^I$, are chosen as special frames from I-frame, P-frame and B-frame in this paper. By combining these two kinds of methods for preprocessing, dependencies among horizontally adjacent pixels in a frame, the intra and inter distortions can be captured sufficiently. The total output frames, $\boldsymbol{F}$, can be expressed as:

Figure 3. Accordion unfolding transformation



$$\boldsymbol{F} = \{F_{k_1}^{'}, F_{k_2}^{I}\}, k_1 \in C_1, k_2 \in C_2 \tag{11}$$

where $C_1 = \{1,2,\cdots,N-2\}, C_2 = \{1,2,\cdots,N/GOP\}$ and N is the number of video frames. The combination of spatial correlation with temporal correlation enhances the detection against DCT/DST-based steganography for HEVC videos.

In short, according to the combination of SFE and AU, the output of the preprocessing of 3D-2D transformation preserves the features of both intra and inter distortions, which enables SRM to detect DCT/DST-based HEVC steganography more effectively.

Feature Extraction and Ensemble Classifier

SRM (Fridrich & Kodovsky, 2012) is introduced to obtain the combination feature. Many filters, including Subtractive Pixel Adjacency Matrix (Pevny et al., 2010), are combined in it. The rich model consisting of diverse sub-models enables the model to detect various embedding distortions. Ensemble classifier (Chen et al., 2012; Kodovsky et al., 2012) consists of L binary classifiers called base learners. It obtains decision by fusing L decisions of individual classifiers using majority voting. It is capable

Figure 4. Combination of special frames extraction and accordion unfolding

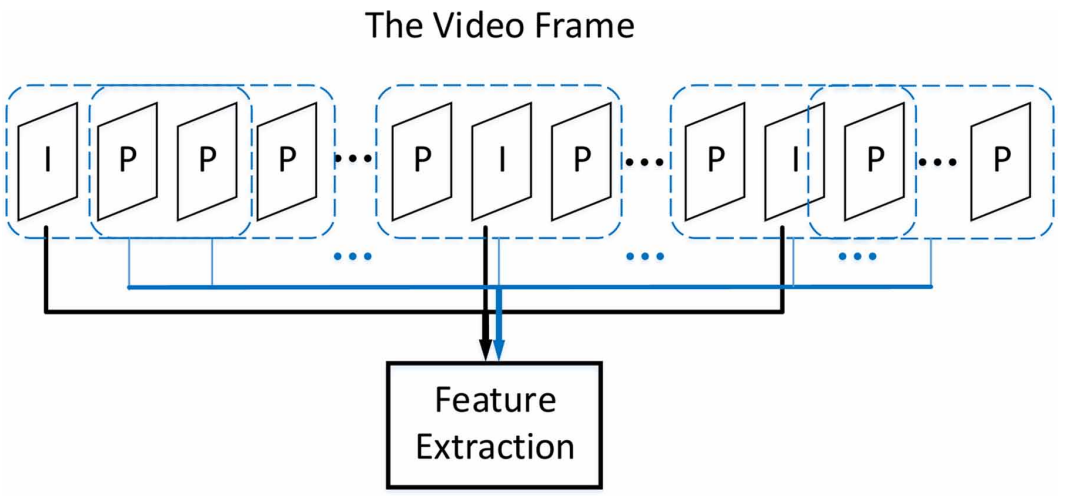


Table 2. Environment of experiments

	Values
Encoder	X265 (ver 2.8)
Decoder	HM 16.7
Different Videos Number	22
Resolution of Sequences	1920 × 1080
Total Frames to be Encoded	11200
GOP Size	10
GOP Structure	IPPP・・・
QP Range	{22, 27, 32, 37, 42}

of dealing with features with high dimension and very large training sets with a low computational complexity, which is hard for SVM classifier. Therefore, it is used as analyzer in this paper.

EXPERIMENTS AND ANALYSIS

Experiments Setup

The details of experiment environment are listed in Table 2. The several steganography algorithms have been implemented in an open source software X265. HEVC is designed for high definition videos to get higher coding efficiency. For this reason, 22 YUV sequences (aspen, blue sky, controlled burn, crowd run, ducks take off, factory, in to tree, life, old town cross, park joy, pedestrian area, red kayak, riverbed, rush field cuts, rush hour, snow mint, speed bag, station, sunflower, touchdown pass, tractor, west wind easy) with 1080P resolution are used in this study. However, not all of these sequences have the same frame numbers. In experiments, in order to determine the number of GOP clearly, all these sequences are further divided into small sequences with 100 frames each, and 112 subsequences are gained. In each experiment, these 22 different videos are encoded into 22 cover videos and 22 corresponding stego videos. Half of them (11 videos) are used for training and other half are used for testing. Spatial only steganalysis (Fridrich & Kodovsky, 2012) and only Accordion Unfolding transformation based steganalysis (Tasdemir et al., 2015), denoted as Fridrich et al. (2012) and Tasdemir et al. (2015), are used for comparison. The latest DCT/DST-based HEVC steganography methods in Chang et al. (2014) and Liu et al. (2018) are used to embed messages, denoted as Liu et al. (2018) and Chang et al. (2014). In order to prove the universality of proposed steganalysis, two kinds of LSB steganography are also used. One of them embeds messages by changing all non-zero QDST coefficients of 4 × 4 blocks in I-frames, denoted as 4 × 4 LSB. The other embeds messages by changing the highest frequency QDCT/QDST coefficients unequal to 0, 1, -1 of all blocks in I-frames, denoted as HF LSB.

Comparison with Other Methods

The optimal settings of ensemble classifier are shown in Table 3. OOB, "out-of-bag" error estimate, is an unbiased estimate of the testing error. The optimal number of base learners L, the dimensionality of each feature subspace etc. parameters are determined automatically during ensemble training for minimizing the OOB error estimate, until it starts showing signs of saturation (Fridrich & Kodovsky, 2012). As shown in Table 3, both optimal number of base learners (Optimal L) and optimal OOB in

Table 3. Performance results obtained during training of different steganography methods. Items marked with * represent steganalysis for comparison

Steganography Method		Liu et al. (2018)	Chang et al. (2014)	4×4 LSB	HF LSB
Optimal L	Fridrich et al.* (2012)	112	105	142	116
	Tasdemir et al.* (2015)	118	109	131	116
	proposed steganalysis	103	101	112	102
Optimal OOB	Fridrich et al.* (2012)	0.3095	0.2582	0.4128	0.2724
	Tasdemir et al.* (2015)	0.3071	0.2547	0.4100	0.2705
	proposed steganalysis	0.2983	0.2451	0.4010	0.2668
Training Time (sec)	Fridrich et al.* (2012)	2.30	2.26	2.86	2.42
	Tasdemir et al.* (2015)	2.41	2.21	2.59	2.38
	proposed steganalysis	2.21	2.22	2.54	2.42

proposed steganalysis are less than other methods against four steganography methods. Less training time is obtained with the decrease of the first two parameters. As shown in the first column of Table 3, when against Liu et al. (2018), optimal L is 103 and optimal OOB is 0.2983 in the proposed steganalysis, leading that just 2.21s is required, which suggests that the proposed steganalysis performs better in the process of training. The novel steganalysis not only shows advantage of attacking steganography algorithms designed in recent years, but also gives an outstanding performance when detecting classical algorithms. As shown in the third column of Table 3, the number of optimal L in the proposed steganalysis has a significant drop compared with other methods. Optimal L is 142, 131 and 112 respectively in three steganalysis methods. Optimal OOB is 0.4010 and training time is 2.54s in the proposed steganalysis, thus the proposed steganalysis presents minimum values in these two parameters among three methods. In short, the novel steganalysis is suitable for many kinds of steganography algorithms. Therefore, while more 2D data need to be dealt with, the proposed steganalysis shows less computational power, less memory and less time for training than other methods.

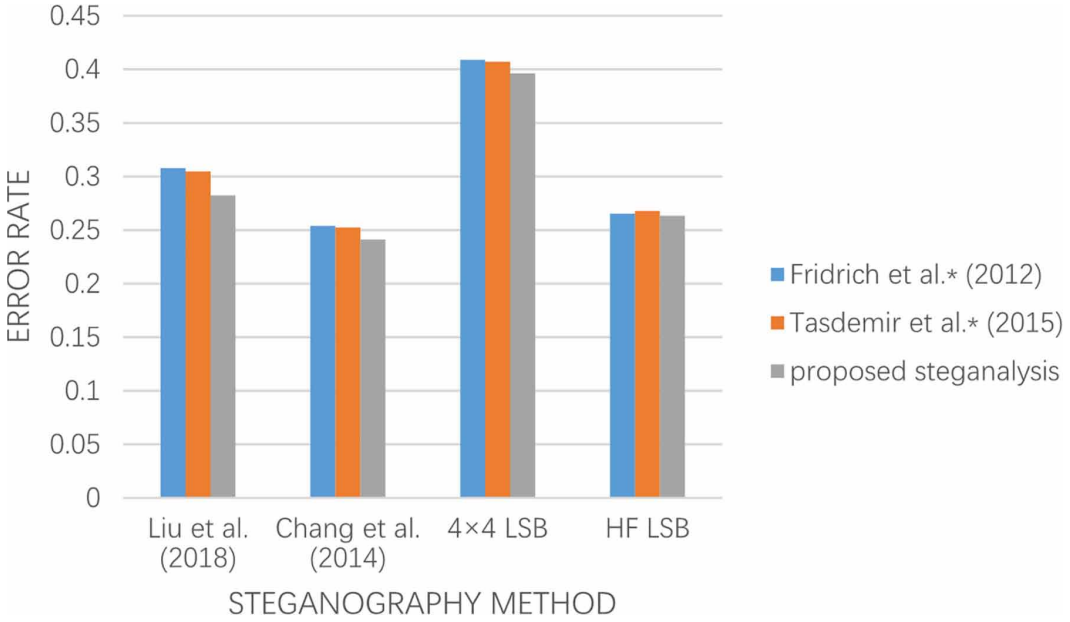
The test results are given in Table 4. The error rate is lower in the proposed steganalysis. As shown in the first column of Table 4, for Liu et al. (2018), error rate in the proposed steganalysis is 0.2824, while Fridrich et al. (2012) shows 0.3079 and Tasdemir et al. (2015) shows 0.3047. In summary, error rate in the proposed steganalysis has 2% decrease compared with other methods. However, while Tasdemir et al. (2015) introduces temporal correlation, it performs worse against HF LSB than Fridrich et al. (2012). As shown in the last column of Table 4, the error rate of 0.2679 is higher than 0.2653, which means that the only AU transformation based method is not always better than spatial only method. Corresponding error rate variation is shown in Figure 5. In Figure 5, the decline trend of error rate in three methods is more visually. In short, the proposed steganalysis using combination feature achieves lower error rate than other methods, which is benefited from the less OOB.

To summarize, the proposed steganalysis requires less computational power and less time for training than other methods. Besides, lower error rate is obtained by using the proposed steganalysis than other methods. Interestingly, the simplest 4×4 LSB is more secure with error rate of 0.3963, as shown in the third column of Table 4. The 4×4 block in HEVC video frames means textured areas and around edges, where the change in pixel is larger and more frequent. Hence the change in pixel caused by embedding with 4×4 LSB is relatively difficult to detect.

Table 4. The value of error rate of different steganography methods. Items marked with * represent steganalysis for comparison

Steganography Method		Liu et al. (2018)	Chang et al. (2014)	4×4 LSB	HF LSB
Error Rate	Fridrich et al.* (2012)	0.3079	0.2540	0.4090	0.2653
	Tasdemir et al.* (2015)	0.3047	0.2525	0.4071	0.2679
	proposed steganalysis	0.2824	0.2412	0.3963	0.2634

Figure 5. Error rate variation of different steganography methods. Items marked with * represent steganalysis for comparison



Comparison With Different QPs

To prove the universality of the conslusions for different QPs, five QPs are examined individually against Liu et al. (2018). As shown in Table 5, optimal L and optimal OOB are less in the proposed steganalysis, yielding less training time. As shown in the second column of Table 5, when QP is 27, optimal L in three methods is 112, 110 and 102 respectively, and optimal OOB is 0.2358, 0.2368 and 0.2297 respectively. Just 2.25s is required for training in the proposed steganalysis under QP of 27. Thus, the novel steganalysis performs better. As shown in the third column of Table 5, when QP is 32, optimal L is 96 and optimal OOB is 0.1623 with only 2.16s required for training. There are still obvious advantages in the proposed steganalysis. In short, the conclusion is the same as the experiment above. Under different QPs, the proposed steganalysis presents less optimal L and optimal OOB as well as less training time. Therefore, despite the change in the value of QP, the proposed steganalysis still performs better than other methods in the process of training.

The test results are presented in Table 6. The value of error rate in the proposed steganalysis is lower under different QPs. As shown in the third column of Table 6, under the QP of 32, the error rate of 0.1584 is lower than 0.1638 and 0.1643. When QP is 37, as shown in the fourth column of Table 6, error rate with proposed steganalysis is only 14.79%. Corresponding error rate variation under different QPs is shown in Figure 6. Intuitively, error rate in the proposed steganalysis is lower than

Table 5. Performance results obtained during training of different QPs

QP		22	27	32	37	42
Optimal L	Fridrich et al. (2012)	112	112	107	95	94
	Tasdemir et al. (2015)	118	110	103	95	98
	proposed steganalysis	103	102	96	95	92
Optimal OOB	Fridrich et al. (2012)	0.3095	0.2358	0.1679	0.1514	0.1598
	Tasdemir et al. (2015)	0.3071	0.2368	0.1676	0.1512	0.1605
	proposed steganalysis	0.2983	0.2297	0.1623	0.1507	0.1539
Training Time (sec)	Fridrich et al. (2012)	2.30	2.40	2.24	1.98	1.98
	Tasdemir et al. (2015)	2.41	2.66	2.54	2.03	2.08
	proposed steganalysis	2.21	2.25	2.16	2.01	2.06

other methods and there is a remarkable decrease in the lower QPs. Besides, with the growth of QP, the error rate tends to decrease. In HEVC video coding, QP is the key to determine video bitstream, and QP is inversely proportional to bit rate. With the increase of QP, bit rate decreases, and video distortion is enhanced, leading to the decline of video quality. Thus, when QP is higher, the error rate tends to be lower. The experimental results show that, under different QPs, the proposed steganalysis gives lower value of error rate than other methods. The use of combination feature of SFE and AU and the way of merging spatial and temporal correlation effectively improve the proposed steganalysis. In short, despite the change of steganography algorithms and QP, the proposed steganalysis has a better performance than other works.

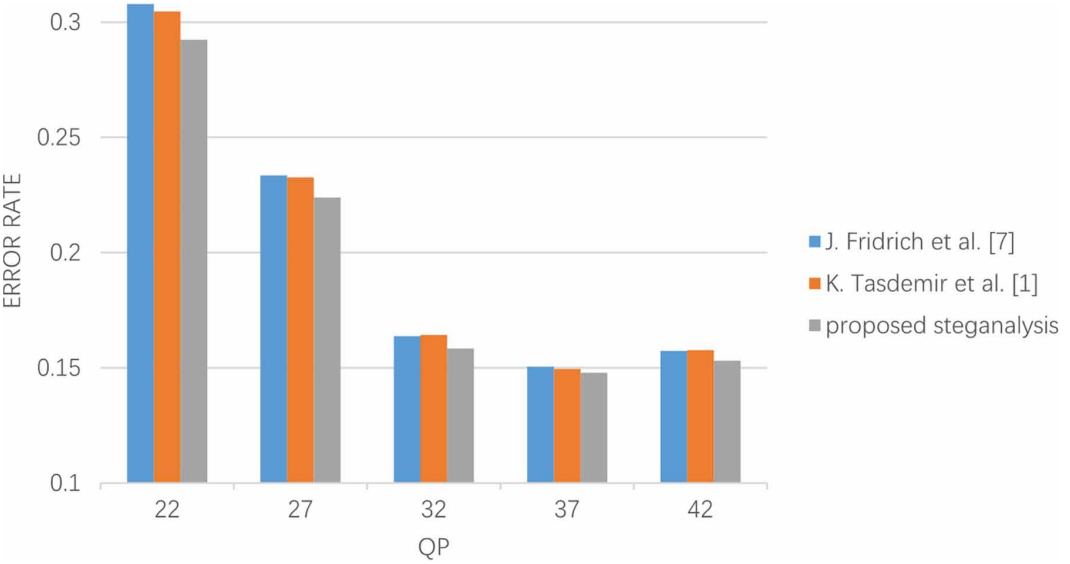
CONCLUSION

In this paper, a novel HEVC steganalysis against DCT/DST-based steganography is proposed. The distortions of DCT/DST-based HEVC steganography are analyzed. Based on the analysis, two kinds of distortion, the intra-frame distortion and the inter-frame distortion, are mainly caused by DCT/DST-based steganography. Aiming at these distortions, the novel HEVC steganalysis is proposed. It utilizes a combination feature of SFE and a temporal to spatial transformation, AU, and merges spatial and temporal correlation. The combination feature of SFE and AU is obtained by preprocessing of 3D-2D transformation. In the experiment, video data sets established from four kinds of steganography algorithms in HEVC are detected, and two kinds of steganalysis methods are introduced for comparison with the proposed steganalysis. The experiments are also done under different QPs. The results of experiments show that the proposed steganalysis performs better than other works. Finding a more effective features extraction method is a future work.

Table 6. The value of error rate under different QPs

QP		22	27	32	37	42
Error Rate	Fridrich et al. (2012)	0.3079	0.2335	0.1638	0.1505	0.1574
	Tasdemir et al. (2015)	0.3047	0.2326	0.1643	0.1495	0.1577
	proposed steganalysis	0.2924	0.2239	0.1584	0.1479	0.1531

Figure 6. Error rate variation under different QPs



ACKNOWLEDGMENT

This work is funded by National Natural Science Foundation of China (Grant No.61572320 & 61572321). It is also supported by the National Key Research and Development Projects of China (2018YFC0830703, 2018YFC0831405). The Corresponding Author is Dr. Tanfeng Sun.

REFERENCES

Babak, S. E., & Akhaee, M. A. (2015). Digital video steganalysis toward spread spectrum data hiding. *IET Image Processing*, *10*(1), 8.

Chang, P. C., Chung, K. L., Chen, J. J., Lin, C. H., & Lin, T. J. (2014). A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames. *Journal of Visual Communication and Image Representation*, *25*(2), 239–253. doi:10.1016/j.jvcir.2013.10.007

Chen, B., Feng, G., & Li, F. (2012). Steganalysis in high-dimensional feature space using selective ensemble classifiers. *Communications in Computer and Information Science*, *331*, 9–14. doi:10.1007/978-3-642-34595-1_2

Da, T., Li, Z. T., & Feng, B. (2015). A Video Steganalysis Algorithm for H.264/AVC Based on the Markov Features. In *Intelligent Computing Theories and Methodologies* (pp. 47–59). Springer International Publishing. doi:10.1007/978-3-319-22186-1_5

Deng, Y., Wu, Y. J., & Zhou, L. N. (2012). Video Steganalysis Exploiting Motion Vector Calibration-Based Features. *Advanced Materials Research*, *482-484*, 168–172. doi:10.4028/www.scientific.net/AMR.482-484.168

Fridrich, J., & Kodovsky, J. (2012). Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, *7*(3), 868–882. doi:10.1109/TIFS.2012.2190402

Holub, V., Fridrich, J., & Denemark, T. (2014). Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security, 1*(1), 1.

Holub, V., & Fridrich, J. (2012). Designing Steganographic Distortion Using Directional Filters. In *IEEE International Workshop on Information Forensic and Security* (pp. 234-239). IEEE.

Kodovsky, J., Fridrich, J., & Holub, V. (2012). Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security*, *7*(2), 432–444. doi:10.1109/TIFS.2011.2175919

Li, S. B., Deng, H. J., Tian, H., & Dai, Q. X. (2014). Steganalysis of prediction mode modulated data-hiding algorithms in H.264/AVC video stream. *Annales des Télécommunications*, *69*(7-8), 461–473. doi:10.1007/s12243-013-0381-8

Liu, Y. X., Liu, S. Y., Zhao, H. G., & Liu, S. (2018). A new data hiding method for H.265/HEVC video streams without intra-frame distortion drift. *Multimedia Tools and Applications*, *78*(6), 6459–6486. doi:10.1007/s11042-018-6320-y

Mishra, R., & Bhanodiya, P. (2015). A review on steganography and cryptography. In *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)* (pp. 119-122). IEEE. doi:10.1109/ICACEA.2015.7164679

Pevny, T., Bas, P., & Fridrich, J. (2010). Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, *5*(2), 215–224. doi:10.1109/TIFS.2010.2045842

Price, D. (2011). *An estimate of infringing use of the internet*. Retrieved from https://www.mendeley.com/catalogue/technical-report-estimate-infringing-internet

Rabee, A. M., Mohamed, M. H., & Mahdy, Y. B. (2017). Blind jpeg steganalysis based on DCT coefficients differences. *Multimedia Tools and Applications*, *77*(6), 7763–7777. doi:10.1007/s11042-017-4676-z

Sheng, Q., Wang, R. D., Wang, B., Li, Q., & Xu, D. W. (2017). Steganography detection algorithm based on the prediction mode correlation for HEVC. *Journal of Optoelectronics Laser*, *28*(7), 766–772.

Sullivan, G. J., Ohm, J., Han, W. J., & Wiegand, T. (2013). Overview of the High Efficiency Video Coding (HEVC) Standard. *IEEE Transactions on Circuits and Systems for Video Technology*, *22*(12), 1649–1668. doi:10.1109/TCSVT.2012.2221191

Tasdemir, K., Kurugollu, F., & Sezer, S. (2015). A steganalysis system utilizing temporal pixel correlation of HEVC video. In *2015 23nd Signal Processing and Communications Applications Conference (SIU)* (pp. 2446-2449). IEEE. doi:10.1109/SIU.2015.7130377

Tasdemir, K., Kurugollu, F., & Sezer, S. (2015). Spatio-temporal rich model for motion vector steganalysis. In *International Conference on Acoustics Speech and Signal Processing (ICASSP)* (pp. 1717-1721). IEEE. doi:10.1109/ICASSP.2015.7178264

Tasdemir, K., Kurugollu, F., & Sezer, S. (2016). Spatio-temporal rich model-based video steganalysis on cross sections of motion vector planes. *IEEE Transactions on Image Processing*, *25*(7), 3316–3328. doi:10.1109/TIP.2016.2567073 PMID:28113715

Wang, P., Cao, Y., Zhao, X., & Wu, B. (2015). Motion vector reversion-based steganalysis revisited. In *2015 IEEE China Summit and International Conference on Signal and Information Processing (China SIP)* (pp. 463-467). IEEE. doi:10.1109/ChinaSIP.2015.7230445

Wang, P., Cao, Y., Zhao, X., & Zhu, M. (2017). A Steganalytic Algorithm to Detect DCT-based Data Hiding Methods for H.264/AVC Videos. In *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security* (pp. 123-133). ACM. doi:10.1145/3082031.3083245

Zhao, Y., Zhang, H., Cao, Y., Wang, P., & Zhao, X. (2015). Video steganalysis based on intra prediction mode calibration. In *2015 International Workshop on Digital-forensics and Watermarking (IWDW)* (pp. 119-33). Springer International Publishing.

Henan Shi is in the school of cyber security, Shanghai JiaoTong University, Shanghai. She is studying for a master's degree. Henan Shi majors in Electronic and Communication Engineering. Her research interests include video steganography and video steganalysis.

Tanfeng Sun received the Ph.D. degree in Information and Communication System from Jilin University, Changchun, P.R. China, in 2003. He is currently an Associate Professor with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, P.R. China. He had cooperated with Prof. Y.Q. Shi in New Jersey Institute of Technology, U.S.A., as a visiting scholar from Jul. 2012 to Dec. 2013. His research includes Digital Forensics on Video Forgery, Digital Video Steganography and Steganalysis, Watermarking, Content Analysis and Intelligence Recognition, and so on. He had published over 140 papers and patents with his colleagues till now. Dr. Sun is an IEEE Senior Member.

Xinghao Jiang received the Ph.D. degree in electronic science and technology from Zhejiang University, Hangzhou, China, in 2003. He was a Visiting Scholar with the New Jersey Institute of Technology, Newark, NJ, USA, from2011 to 2012. He is currently a Professor with the Institute of Cyber Space Security at Shanghai Jiao Tong University, Shanghai, China. His research interests include multimedia security and image retrieval, intelligent information processing, cyber information security, information hiding and watermarking. Dr. Jiang is an IEEE member.

Yi Dong received the B.S. degree from Shanghai JiaoTong University, Shanghai, China. He is currently pursuing the Ph.D. degree with the school of cyber security, Shanghai JiaoTong University, Shanghai. His research interests include video steganography and video steganalysis.

Ke Xu received the Ph.D. degree in the Institute of Cyber Space Security from Shanghai Jiao Tong University, Shanghai, China, in 2019.He is currently a post doctor in the Institute of Cyber Space Security, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His research interests include action recognition, abnormal events detection, and gait recognition. Dr. Xu is an IEEE member.